Using PCP (RFC6887) with CoAP endpoints

Jaime Jiménez
jaime.jimenez@ericsson.com

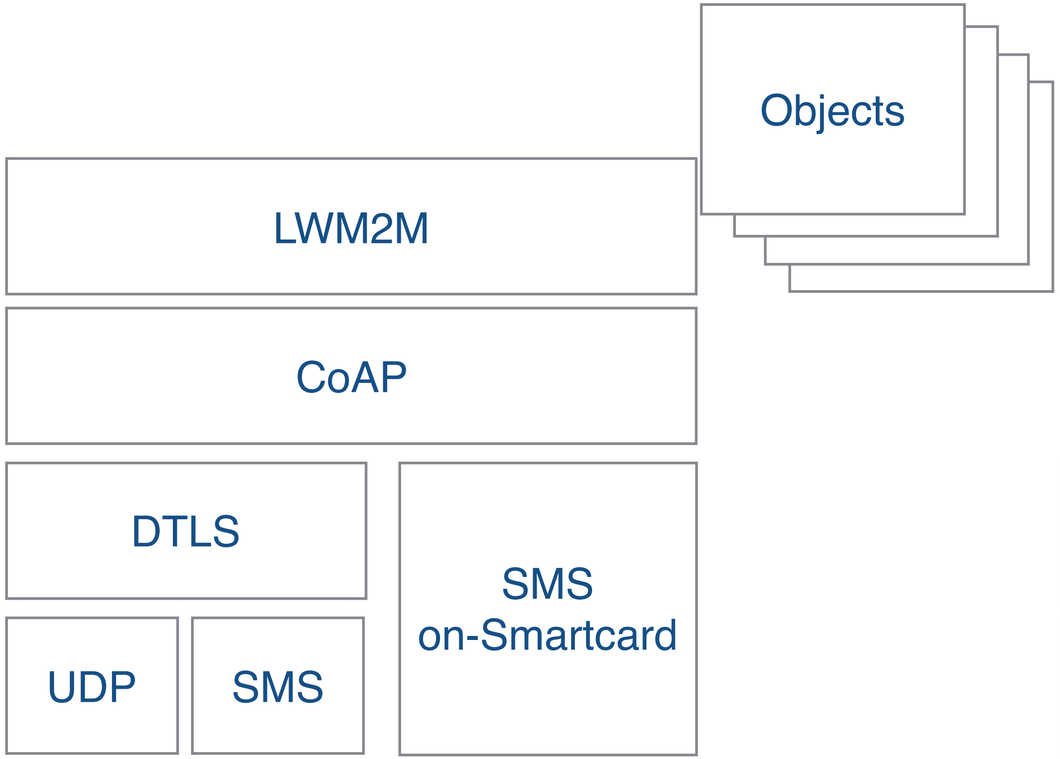
@jaim - jaimejim.github.io

ERICSSON

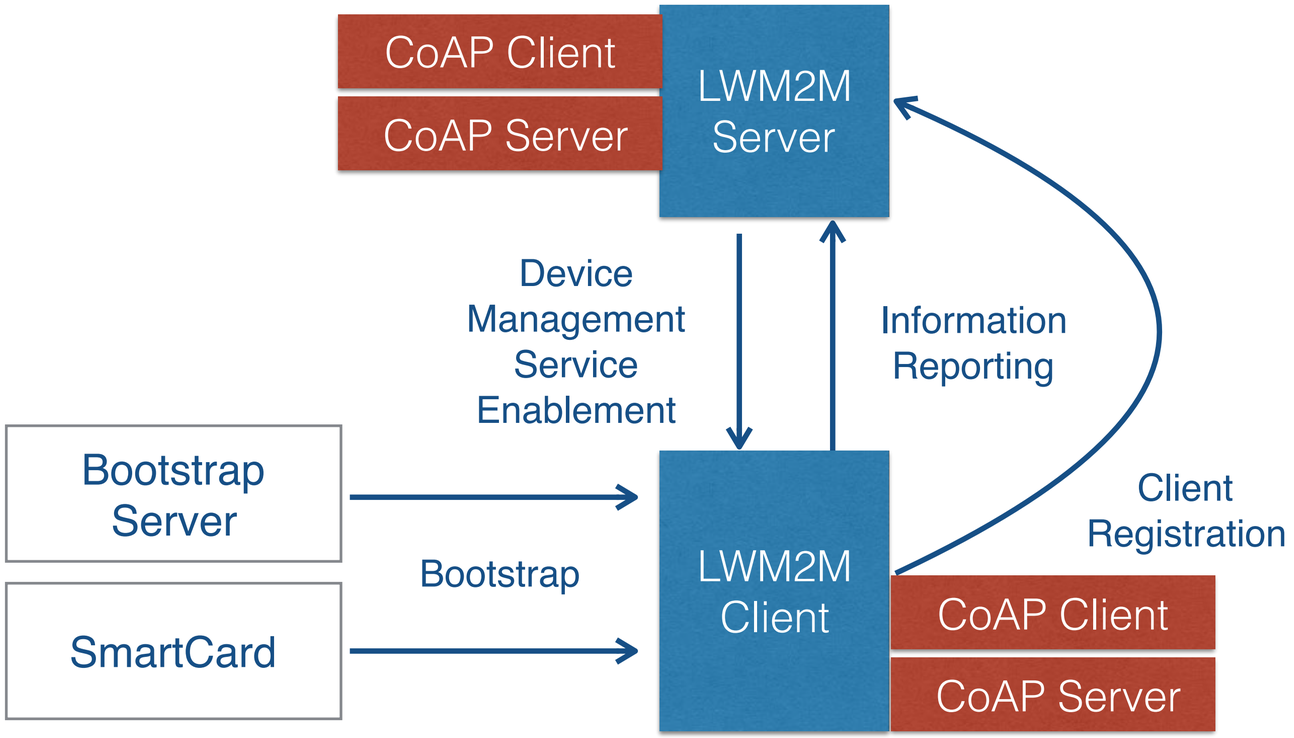
Problem Statement

- NATs and Firewalls are an issue for constrained devices.
- There does not seem to be one single solution to the problem.

Managed Devices with LWM2M



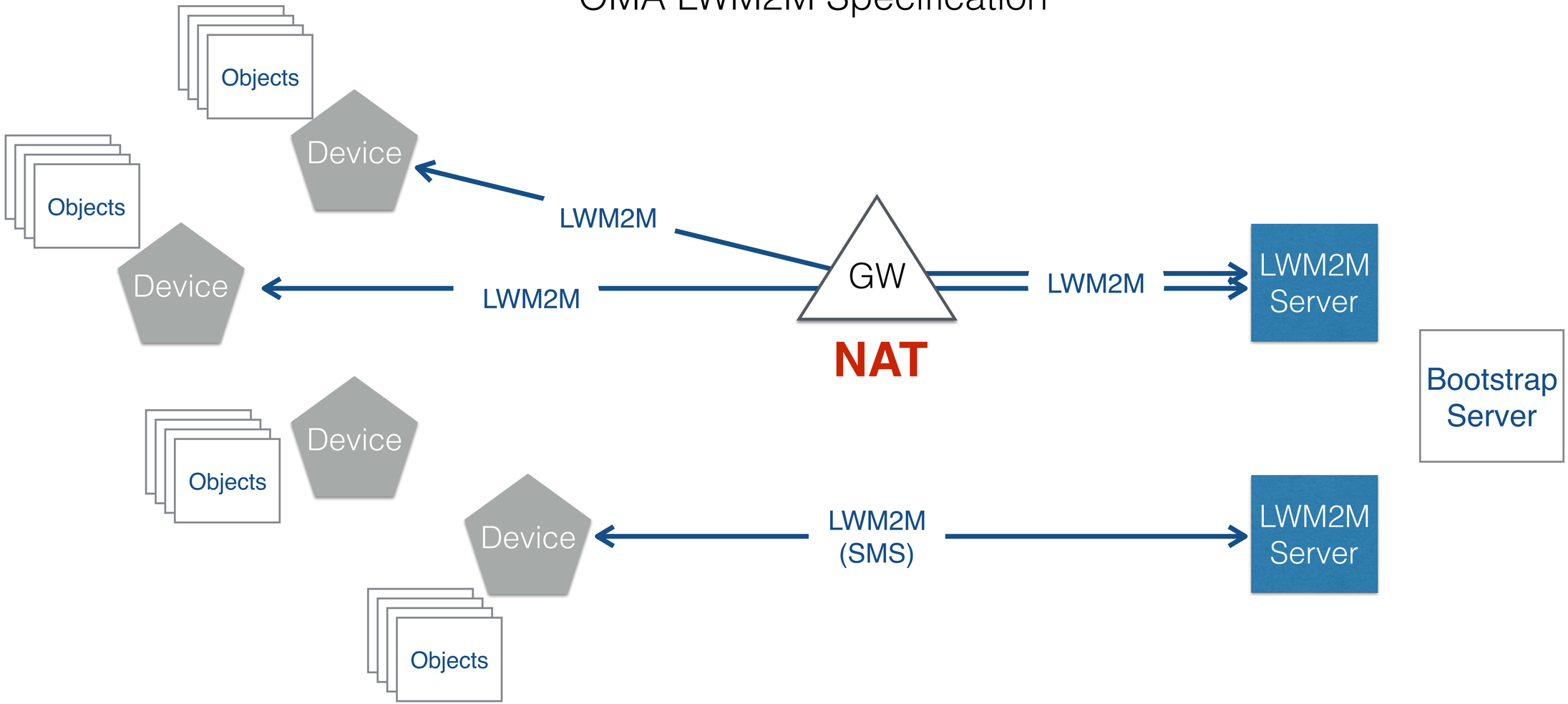
LWM2M Device Stack



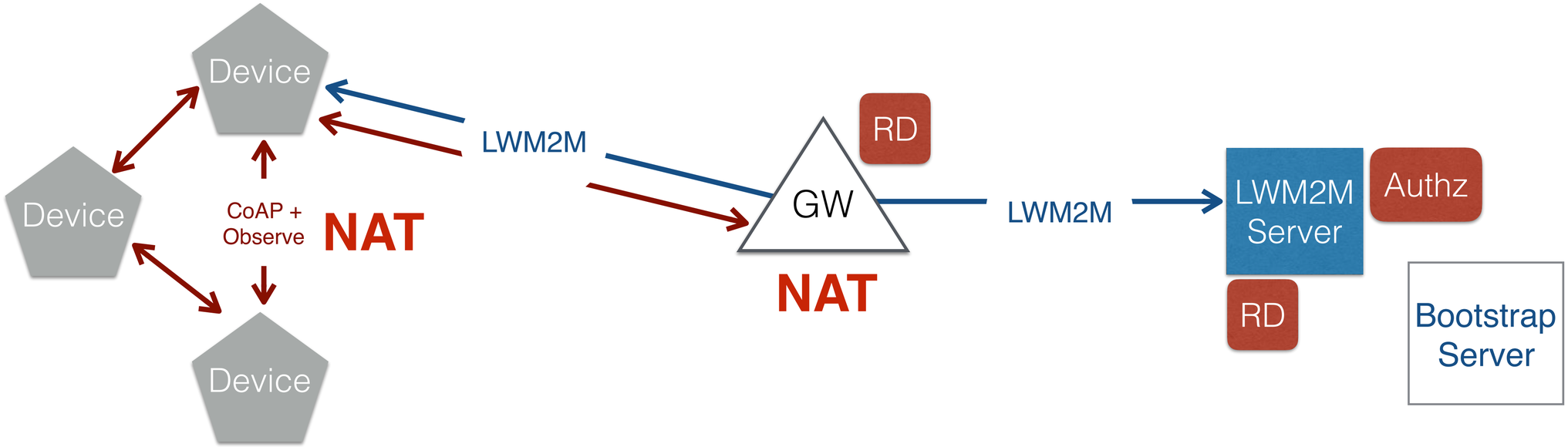
LWM2M Architecture

LWM2M Interactions

OMA LWM2M Specification



Interactions among CoAP EPs



Common solutions

1. Sending messages (either inside or outside of network) for punching holes in the NAT (PINGs, Keepalives…).
2. IPv6
3. Session Traversal Utilities for NAT (STUN), RFC5389
4. Socket Secure (SOCKS).
5. Traversal Using Relays around NAT (TURN) is a relay protocol designed specifically for NAT traversal.
6. Interactive Connectivity Establishment (ICE) and STUN.
7. UPnP Internet Gateway Device Protocol (IGDP).
8. NAT-PMP as an alternative to IGDP.
9. Port Control Protocol (PCP) as alternative to NAT-PMP, RFC6887.
10. Application-level gateway (ALG).

Common solutions

1.Sending messages (either inside or outside of network) for punching holes in the NAT (PINGs, Keepalives…).

constrained in battery

2.IPv6.

ideal

3.Session Traversal Utilities for NAT (STUN), RFC5389

4.Socket Secure (SOCKS).

5.Traversal Using Relays around NAT (TURN) is a relay protocol designed specifically for NAT traversal.

6.Interactive Connectivity Establishment (ICE) and STUN.

7.UPnP Internet Gateway Device Protocol (IGDP).

updated

8.NAT-PMP as an alternative to IGDP.

updated

9.Port Control Protocol (PCP) as alternative to NAT-PMP, RFC6887.

10.Application-level gateway (ALG).

complex

Basic Idea

Use standard PCP to signal the NAT.

+	-
Simple standard solution.	NAT configurations vary.
Added benefit of configuring firewalls too.	Firewall configurations too.
Low overhead and no keepalives.	Not much info on deployed NATs (to my knowledge)
No need for other transports than UDP.	
No need for other servers.	

General Operation in LWM2M

1. The LWM2M Client requests Bootstrap to LWM2M Bootstrap Server (BS).

2. BS overwrites the information on the device.

3. A new LWM2M Object named PCP-context is created. Details about the Object are below.

4. LWM2M Client registers on server.

5. If binding is U and Queue mode is needed the LWM2M Server can enable PCP.

6. The Server sets the values for the lifetime and checks the appropriate version on the client.

7. The LWM2M client sends first a PCP request to the default gateway (the one that provided the DHCP6 resolution) on port 5351.

8. If no response is received the Client then tries the default Anycast address 2001:1::1/128 and awaits a response.

9. When a response is received the state of the PCP Object should change and a notification to the LWM2M server MAY be sent to confirm that PCP is enabled.

To be done

- Find out current deployment of PCP, specially on home gateways.
- Work out first draft (WIP), LWIG, CORE.
- Beyond basic cases.
    - How to forward config to other NATs in between.
    - How to delegate to other endpoints.
    - Use of extra PCP features like MAP and PEER Opcodes.
    - Measurements of complexity and traffic.